PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06F 1/00, 13/00	A1	(11) International Publication Number: WO 98/53384
		(43) International Publication Date: 26 November 1998 (26.11.98)

<table>
<tr><td>

(21) International Application Number: PCT/SE98/00948

(22) International Filing Date: 20 May 1998 (20.05.98)

(30) Priority Data:
9701894–9   21 May 1997 (21.05.97)   SE

(71) Applicant (for all designated States except US): TELEFONAK-TIEBOLAGET LM ERICSSON [SE/SE]; S–126 25 Stockholm (SE).

(72) Inventor; and
(75) Inventor/Applicant (for US only): CARLSUND, Peter [SE/SE]; Lilla Sällskapets väg 75, S–127 61 Skärholmen (SE).

(74) Agents: HERBJØRNSEN, Rut et al.; Albihns Patentbyrå Stockholm AB, P.O. Box 3137, S–103 62 Stockholm (SE).

</td><td>

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, GW, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

</td></tr>
</table>

(54) Title: METHOD AND APPARATUS FOR ACTIVATING PROGRAMS/FEATURES IN A COMPUTER

(57) Abstract

A method and an apparatus for handling the access to optional features in a computer system, such as a telephone exchange, are disclosed. The computer system comprises an encryption key. Each feature is associated with a feature identification integer (FI), a feature activation integer (FA) and a data tag (FD). To activate a feature, the user enters a number of integers, received from the system vendor and encrypted using the same encryption key found in the computer system. The integers are decrypted, an arithmetic operation performed, and the result compared with the integers associated with the feature. If there is a match, the feature is activated, forever, or for a period of time determined by the integers. The use of features may be stored in a log (11), which may, together with a log indicator (9), be used by the vendor to check the use of optional features.

METHOD AND APPARATUS FOR ACTIVATING PROGRAMS/FEATURES IN A COMPUTER

Technical Field

The present invention relates to computer systems and especially to the handling of

5   optional features in such systems.

Background

Especially in large computer systems, there is a need for vendors to offer optional

functions or features that can be made available to an operator if and when they are

10   paid for. In many cases the original order does not include these features. This

means that the additional order of such functions will result in a software delivery

procedure. The procedure to create the software package, deliver it to the customer

and upgrade the target system is costly and time consuming. Installation also

requires that the system be taken down while the software is installed.

15

Also the system management becomes increasingly difficult when new deliveries are

made.

Often customers want to test a feature over a period of time before deciding whether

20   or not to buy it. This normally requires test installation of programs.

One example of such a computer system is a modern digital telephone exchange. In

telephone exchanges it is particularly important to avoid service interrupt. Therefore,

there is a strong desire to be able to change the functionality of a telephone exchange

25   without having to take the exchange out of service.

One solution is to deliver a complete software system to the customer, but to activate

only the programs or features the customer has ordered. The other programs or

features could then be activated at a later date without new software installation.

30

Sometimes a licence principle is used and the target system has special software for managing licence registration and licence supervision to prohibit illegal installation and utilization of that software.

5   For licence management a solution known as hardware keys is often used, mostly by vendors of personal computers (PCs). Hardware keys are delivered to the customer together with the software and connected to a serial port on the computer, normally the printer port. The delivered software comprises a unique built-in key which can only be activated by the hardware key. As the software cannot operate without the

10   hardware key, the software is in effect protected from unauthorized copying.

A method to prevent continued unauthorized use of protected software when a testing time has elapsed is disclosed in US-A-5,014,234. A set of registration data appended to a selected system file is employed instead of data being a part of the

15   software to be protected. When the proprietor of the protected software receives the registration data, a "diffuse" number is generated from the software serial number and returned to the user.

A method for protecting the distribution of computer programs within a broadcast

20   medium is disclosed in US-A-5,416,840. This means distributing a large number of different software titles to a large number of potential customers, for instance on CD-ROM. Each stored encrypted program has an associated identifier that may be used to identify a selected program on the medium. The system has a decrypting device which has an associated unique identifier.

25

Two tables are generated and stored. The first table includes the correlations between the encryption key and the program identifier. The second table includes correlations between a password key and the hardware identifier. When a user selects a particular software program from the medium, a program identifier and a

30   hardware identifier are used to permit access to the selected program. In the

document it is foreseen that this will be associated with an obligation to pay for the use of the program.

The solutions described above may be used for complete tools and applications, but
5   are not implemented for special features within the applications.

Summary of the Invention
Thus, it is an object of the present invention to be able to extend the system functionality, in particular in large computer systems, without the need for new
10   software deliveries.

It is another object of the invention to be able to discover any unauthorized use of features in the system without the use of additional hardware.

15   It is yet another object of the invention to provide time-limited test licences of applications or features without the need for new software deliveries.

These objects are achieved according to the invention by equipping the computer system with an encrypting key, which may be unique to one particular system or, if
20   the customer has several similar systems, to a particular customer. This encrypting key is added at system generation and may therefore be invisible to the users of the system. In addition, for each optional feature there is a date tag used for recording the date when the feature status was last changed, one integer identifying the feature and one integer identifying the activation status of the feature. The two integers are
25   stored as encrypted values, encrypted using the site unique encoding key. One particular feature is always identified by the same integer in all systems, but this integer will be stored in the systems encrypted with different encrypting keys.

When a feature is to be activated, as negotiated between the vendor and the
30   customer, the vendor sends at least two integers to the customer, encrypted using the same encrypting key as the one found in the customer's system. The customer enters

these integers into his system. The system decrypts the integers and performs one or more arithmetic operations, to determine if the entry is valid, what feature should be activated and for how long. An electronic seal may be used to confirm that the delivery had been authorized by the vendor.

5

In the log, the use of features is logged together with other information about activities that occur regularly in the system, for example about system restarts. In this way, the log is never empty, and log entries occur regularly, unless the log or the logging function has been tampered with. Thus, if someone tries to cheat, it will be
10   revealed in the log.

The invention offers the following advantages:
The method according to the invention enables the installation of all features at an initial installation.

15

The log enables the vendor to check what features the customer has used since installation.

The log enables the vendor to check that only activated features have been used and
20   that all activation procedures were the result of appropriate business transactions.

The logging of routine activities together with the information about the activation/deactivation of features allows the vendor to check if the logging function and/or the log file has been tampered with.

25

The security level of the method according to the invention is such that unauthorized activation of features will be possible if the system is tampered with. Also, no automatic deletion or deactivation of services is foreseen. However a logging function allows the system vendor to identify unauthorized use of features.
30   Therefore, the method according to the invention is suitable for large systems or

systems with a relatively small number of customers, when the vendor and the customer maintain contact throughout the system's lifetime.

Brief Description of the Drawings

5   The invention will be described in more detail in the following, with particular reference to the drawings, in which:

Figure 1 is a schematic representation of a computer system according to the invention;

Figure 2 is a flowchart of the events that occur when a feature is to be activated in a
10   system according to the invention;

Figure 3 is a flowchart of the events that occur when someone tries to use an optional feature in a system according to a preferred embodiment of the invention.

Detailed Description of the Embodiments

15   Figure 1 is a schematic representation of a computer system according to the invention. The system comprises a number of basic functions 1, for example an operating system, or, in a telephone exchange, the basic switching functions and the basic subscriber functions. The system also comprises an encrypting key 3, which is unique to the system, and which is included when the system is manufactured. Since
20   the encrypting key is added at the initial system generation, it is neither logged nor visible outside the system. However, it is known at the central managing site, from which new features are purchased.

There are one or more optional programs and/or features F1, F2, ... , Fn within the
25   programs. As an example, consider an office program package containing a spread sheet, a word processing programming, and file managing program. The word processing program has some optional features, such as a graphics package and an equation editor. If the customer wants only the file managing program and the basic version word processing program, the whole package would be delivered, but the
30   spread sheet program, the graphics package and the equation editor would be locked, or deactivated. Later on, if the customer wanted the graphics functions, it would

already be available without any new installation, and would only need to be activated.

If the computer system is a telephone exchange, for example, it may include the

5   basic subscriber services from the beginning, but not optional features such as call waiting and call forwarding, which may be offered to the subscribers, and which may be wanted at a later stage.

Each optional feature F1, F2, ..., Fn comprises the feature software FSW and three

10   integers, encrypted with the system unique encrypting key, to be used when the service is activated: one feature date tag FD, one feature identification number FI and one feature activation status FA.

When a feature is to be activated, the vendor sends at least two integers to the

15   customer, which are to be entered into the system. For this and other purposes the system comprises at least one input terminal 5, from which the user can enter the integers. The system also comprises a comparison means 7 for comparing the entered integers with the ones stored in connection with each feature. The use of these integers is discussed in detail in the description of figure 2. In the following

20   discussion of the invention, three integers will be used.

The system includes one log indicator 9 stored in such a way that it is not persistent, for example in the random access memory (RAM). In this log indicator it is indicated at least when a feature is used for the first time. The log records are then

25   written to a log 11 stored on disk, out of reach for the user, so that it cannot be changed or erased manually, as explained in connection with figure 3. It will not be possible to prevent this with 100% certainty, but if attempts to change or erase the log are made, these attempts will leave traces.

30   When a feature is activated, the feature identity, time of activation, activation state and the seal are logged.

If the system is restarted, the log indicator 9 is erased, but the log 11 is not. When the system is powered up or restarted, some system-specific information that is always present and can be verified against other information sources, is checked and

5   stored in the log. In a preferred embodiment, the activation status, and the time and date of the last change of status, of all optional features are registered.

Theoretically it would be possible to log every time a feature is used, but in many cases this would make the log very big and not add any useful information. In some

10   cases the only point of interest, as will be discussed later, is whether or not the customer is using a particular feature, not how many times it is used. To prevent unauthorized persons from tampering with the file it is suggested to let the log consist of a number of sequential files, and to use a wrap-around principle, so that when it is full, the oldest file will be overwritten.

15

The system vendor may examine the log 11 at regular or irregular intervals, to verify that only the features paid for have been used.

The system may further comprise a table 13 for storing previously used integer

20   combinations to prevent later use of the same integers.

Figure 2 shows the events that occur when a feature is to be activated according to a preferred embodiment of the invention. When the feature is purchased, the customer receives at least two encrypted integers from the vendor. In a preferred embodiment

25   three integers I1, I2, I3 are used, which are delivered with an electronic seal. The first two integers I1, I2 are used to identify the feature to be activated and the third integer is used together with the other two, to determine the activation time. It will be obvious to the person skilled in the art that the number of integers used in the operations could be increased. The seal is unique to this business transaction, and

30   may for example be an integer. It is used to verify that the delivery was actually sent from the vendor and that it has not been manipulated by anyone.

As an additional check, the identity of the feature to be activated might be specified in connection with entering the encrypted integers.

5   Step 100: The three integers I1, I2, I3 are entered into the system, normally by the customer.

Step 102: The system decrypts the two first integers I1, I2, using the system unique decrypting key and performs an arithmetic operation on I1 and I2 to produce a new integer I4.

10 Step 104: Is I4 equal to the feature identity FI? If yes, go to step 108; if no, go to step 106.

Step 106: Register the failed attempt to activate the feature in the security log. End procedure.

Step 108: The system decrypts the third integer I3 using the system unique
15 decrypting key.

Step 110: The system performs an arithmetic or Boolean operation on I3 and I4 to produce the activation code A1.

Step 112: Is the activation code A1 equal to zero? If yes, go to step 118; if no, go to step 114.

20 Step 114: If $0<A1\leq365$, go to step 116; otherwise go to step 106.

Step 116: Activate the feature for a number of days corresponding to the value of A1. Go to step 120.

Step 118: Activate the feature permanently. Go to step 120.

Step 120: Set the date tag to the current date and log the activation of the feature.

25

The security log is not necessarily a separate log, but may be part of the log 11.

The arithmetic operations in steps 102 and 104 may be the same kind of operation or different ones. For example, an exclusive or operation may be performed on the
30 binary representation of the two numbers. It will be obvious to the skilled person

that any number of integers might be used in the operations. In step 120 the activation status of the feature may be stored in a log, or in connection with each feature.

5   Figure 3 shows the events that take place when someone tries to use an optional feature in the system. In the example of the computer system|comprising an office program package, this may be when someone tries to run one of the programs or, assuming that a person is working in the word-processing program, for example at an attempt to use the graphics part of the program. In the example of a telephone

10   exchange, it may be when a subscriber tries to use the call forwarding feature.

Step 150: An attempt is made to access a feature.

Step 152: The system checks if the feature has been activated, i.e. if the value of the activation code A1 is within the allowed range (0-365). If yes, go to step 154; if no,

15   go to step 158.

Step 154: The system checks if the activation code A1 equals 0. If yes, go to step 160; if no, go to step 156.

Step 156: The system checks if the activation date of the feature + A1 is less than or equal to today's date. If yes, go to step 160; if no, go to step 158.

20   Step 158: Access to the feature is denied. End of procedure.

Step 160: The system checks if the log indication for the feature is activated. If yes, go to step 166; of no, go to step 162.

Step 162: The system creates a log record comprising the feature identity, activation status and current date in the log indication found in RAM.

25   Step 164: The log record is stored in the log on disk.

Step 166: Access to the feature is granted. End of procedure.

After or in connection to step 158 of course the failed attempt to access the feature could be logged, although this is not shown in the flow chart.

30

After the limited period of time has expired, it would of course be possible to deactivate the feature again by changing the value of the activation status FA to a number outside the allowed range (0-365). In this case, the activity in step 156 might be omitted.

5

Instead of making the feature available for a limited period of time, it would be possible to allow the user to test the feature a limited number of times. This could be solved in different ways; for example, the date tag would be replaced by a field registering the number of times the feature may be used, and a field registering how many times the feature had actually been used. In steps 152, 154, 156, the values of these two fields would be compared. Another possible solution would be to register the number of times the user was allowed to use the feature in a counter field and decrement the value of this counter field each time the feature was accessed.

CLAIMS

1. A method for controlling activation and/or deactivation of programs or parts of programs in a computer system, comprising at least one optional program and/or
5   program part and an encrypting key, each optional program or program part being associated with at least one integer number, **characterized** in that it comprises the following steps

- Manually entering at least one integer (I1), encrypted with the same kind of
10   encrypting key as the one found in the computer system;
- Automatically decrypting the integers using the encrypting key;
- Automatically performing an arithmetic operation on the at least one integers (I1) to produce at least another integer (I4) and comparing the result with a feature identification (FI);
15   - If said second integer (I4) equals said feature identificaton (FI), performing the following steps:
    - performing another arithmetic operation on the same integer or integers (I1) and at least one additional integer (I2) entered into the system, to determine the length of the period for which the feature should be activated.
20   - activating the feature for the specified period of time.

2. A method according to step 1, **characterized** in that the following steps are carried out by the system when an attempt to use the feature is carried out:
- checking if the feature has been activated;
25   - if the feature has been activated, checking if the activation is still valid
- if the activation is still valid, granting access to the feature.

3. A method according to claim 1 or 2, **characterized** in that the feature identity (FI) and the activation time (FD) are stored in a log (11) persistently stored in the system
30   when the activation status of the feature is changed.

4. A method according to claim 3, **characterized** by

- Delivering the integers (I1, I2) to the customer together with an electronic seal, unique to the transaction

- Storing the transaction unique seal in the log (11) when the activation status of the feature is changed.

5. A method according to claim 2, 3 or 4, **characterized** in that the following steps are performed by the system when a valid activation has been verified, but before access to the feature is granted:

- checking if there is a log record for the feature, and, if there is not, performing the following steps:

    - registering the activation of the feature in the log indication (9)

    - creating a log record for the feature and storing it in the persistent log (11).

6. A method according to any of the preceding claims, **characterized** by including an encryption key in the computer system at system generation.

7. A method according to any of the preceding claims, **characterized** in that the computer system is a digital telephone exchange.

8. A computer system comprising one ore more basic functions (1), one or more optional programs and/or program parts (F1, F2, ..., Fn), an encrypting key (3), and means (7) for performing at least one arithmetic operation on at least two integers entered into the system, to produce a result (I4), **characterized** in that each optional program or program part (F1, F2, ..., Fn) is associated with at least one integer (FI), stored encrypted with the encrypting key (3) and that the system comprises means (7) for comparing the result of said at least one arithmetic operation with said at least one integer (FI) and activating the program part if there is a match.

9. A computer system according to claim 8, comprising a log (11), stored in such a way that it cannot be erased in normal operation and that it will remain over a system restart, **characterized** in that said log (11) is adapted to comprise at least information about the activation status (FA) of features, the time (FD) when the activation status of the feature was last changed, the seal, if any, used in the transaction when the activation status was changed, and information about system restarts.

10. A computer system according to claim 8 or 9, **characterized** in that it comprises a log indication file (9) stored in a non-persistent way and adapted to contain information for each feature (F1, F2, ..., Fn) about whether or not the feature has been used.
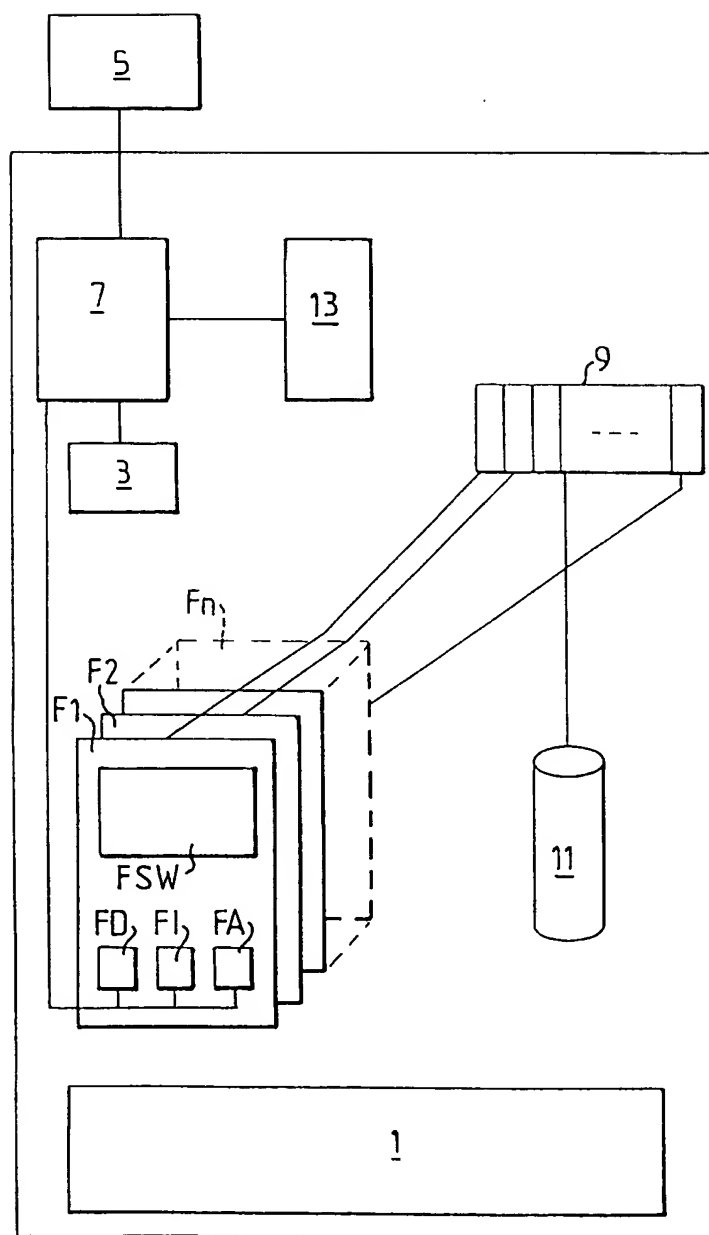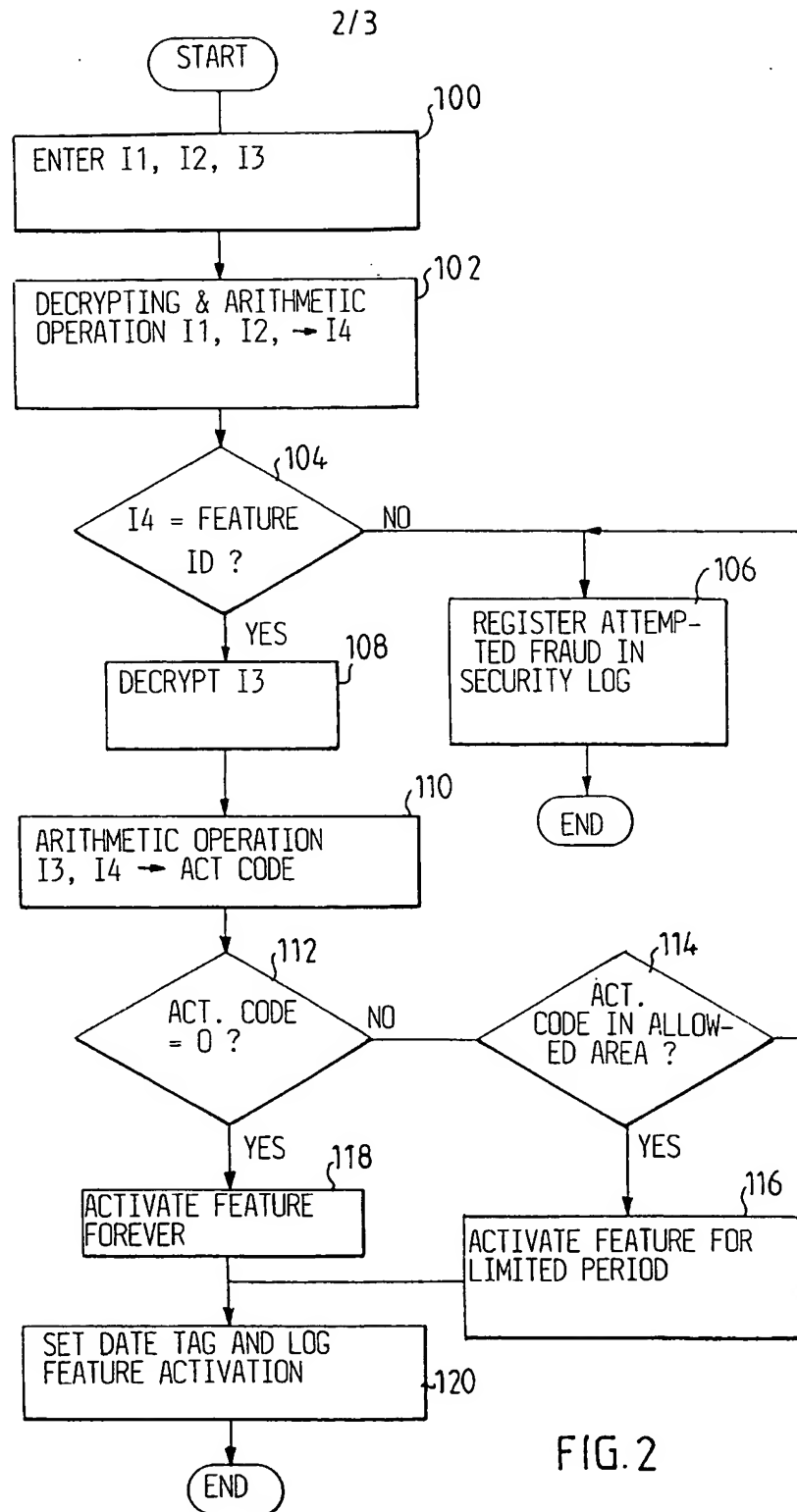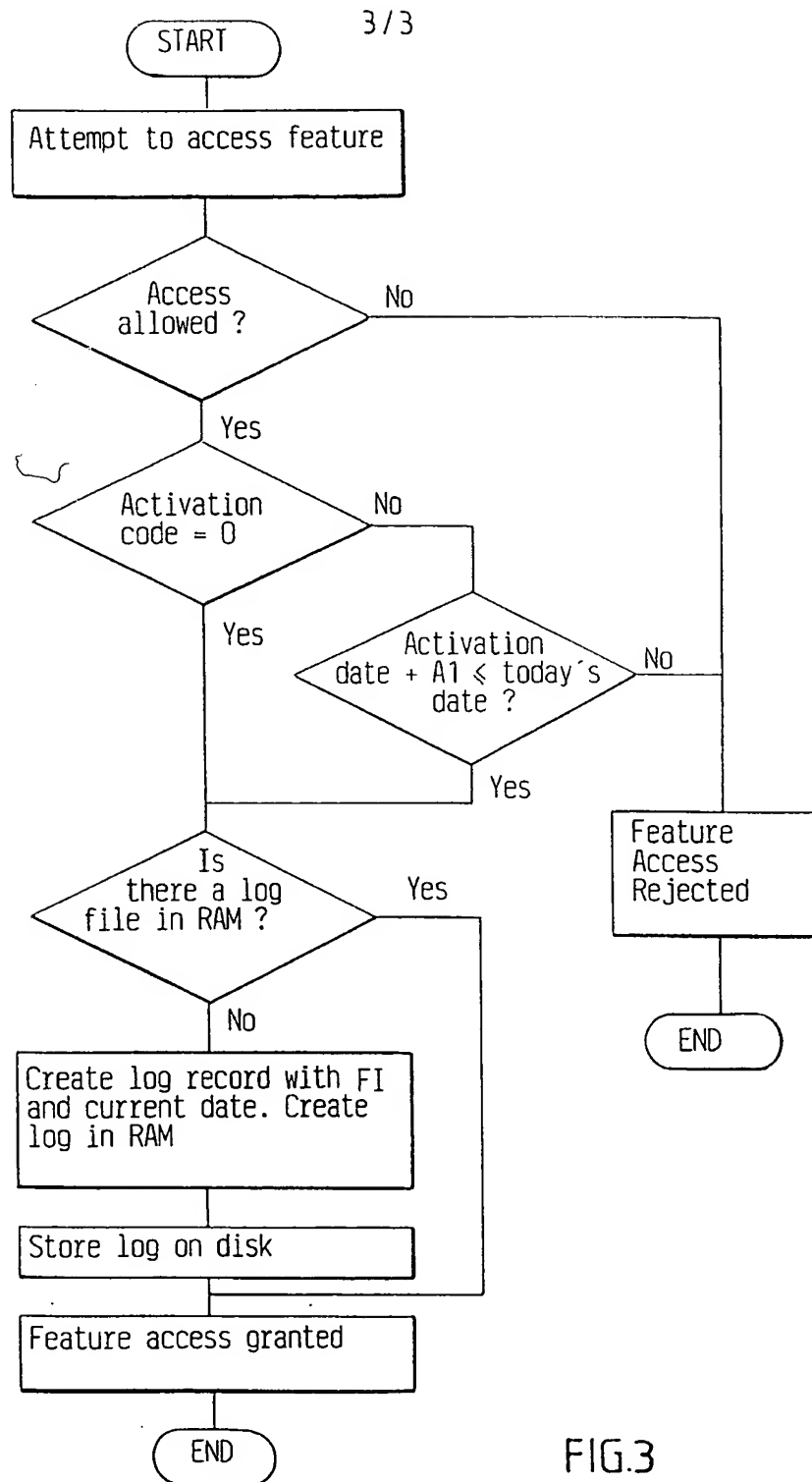
FIG.1

2/3

```
                    ┌──────────┐
                    │  START   │
                    └────┬─────┘
                         │
              ┌──────────▼──────────┐  ⌐100
              │  ENTER I1, I2, I3    │
              └──────────┬──────────┘
                         │
              ┌──────────▼──────────┐  ⌐102
              │ DECRYPTING & ARITH- │
              │ METIC OPERATION     │
              │ I1, I2, → I4        │
              └──────────┬──────────┘
                         │
                    ⌐104 ▼
                   ╱──────────╲          NO
                  ╱  I4 = FEATURE╲──────────────┐
                  ╲    ID ?     ╱               │
                   ╲──────────╱                 │
                        │ YES                    ▼
                        │              ┌──────────────────┐  ⌐106
                   ⌐108 ▼              │ REGISTER ATTEMP- │
              ┌───────────┐           │ TED FRAUD IN     │
              │ DECRYPT I3│           │ SECURITY LOG     │
              └─────┬─────┘           └────────┬─────────┘
                    │                          │
              ⌐110  ▼                          ▼
      ┌────────────────────┐            ┌──────────┐
      │ ARITHMETIC OPERATION│            │   END    │
      │ I3, I4 → ACT CODE  │            └──────────┘
      └──────────┬─────────┘
                 │
            ⌐112 ▼               NO       ⌐114
           ╱──────────╲                  ╱──────────╲
          ╱ ACT. CODE  ╲────────────────╱   ACT.     ╲
          ╲  = 0 ?     ╱                ╲ CODE IN ALLOW-╲
           ╲──────────╱                 ╲ ED AREA ?   ╱
                │ YES                     ╲──────────╱
                │                              │ YES
           ⌐118 ▼                         ⌐116 ▼
    ┌─────────────────┐          ┌──────────────────┐
    │ ACTIVATE FEATURE│          │ ACTIVATE FEATURE │
    │ FOREVER         │          │ FOR LIMITED PERIOD│
    └────────┬────────┘          └────────┬─────────┘
             │                            │
             ▼◄───────────────────────────┘
    ┌─────────────────┐
    │ SET DATE TAG AND│
    │ LOG FEATURE     │  ⌐120
    │ ACTIVATION      │
    └────────┬────────┘
             │
        ┌────▼────┐
        │   END   │
        └─────────┘
```

FIG.2

3/3

FIG.3

1

INTERNATIONAL SEARCH REPORT

A. CLASSIFICATION OF SUBJECT MATTER

IPC6: G06F 1/00, G06F 13/00
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC6: G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPI

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5337357 A (CHOU ET AL), 9 August 1994 (09.08.94), column 4, line 47 - column 5, line 4; Drawing. --	1-10
Y	US 5014234 A (EDWARDS, JR.), 7 May 1991 (07.05.91), abstract --	1-10
Y	US 5023907 A (JOHNSON ET AL), 11 June 1991 (11.06.91), column 4, line 19 - line 25 --	5,9,10
A	US 5182770 A (MEDVECZKY ET AL), 26 January 1993 (26.01.93) --	1-10

[X] Further documents are listed in the continuation of Box C.	[X] See patent family annex.

Date of the actual completion of the international search	Date of mailing of the international search report
5 November 1998	0 9 -11- 1998
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Sylvain Dunand Telephone No. +46 8 782 25 00

BEST AVAILABLE COPY

INTERNATIONAL SEARCH REPORT

International application No.

PCT/SE 98/00948

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 9013865 A1 (SOFTEL, INC.), 15 November 1990 (15.11.90)	1-10
	--	
A	WO 9209160 A1 (TAU SYSTEMS CORPORATION), 29 May 1992 (29.05.92)	1-10
	--	

INTERNATIONAL SEARCH REPORT

Information on patent family members

05/10/98

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5337357 A	09/08/94	CA 2120816 A EP 0636962 A	18/12/94 01/02/95
US 5014234 A	07/05/91	CA 1267443 A	03/04/90
US 5023907 A	11/06/91	NONE	
US 5182770 A	26/01/93	NONE	
WO 9013865 A1	15/11/90	AT 143511 T AU 641397 B AU 5646490 A CA 2053261 A CN 1048271 A DE 69028705 D,T EP 0478571 A,B JP 4504794 T US 5388211 A US 5497479 A US 5613089 A US 5649187 A	15/10/96 23/09/93 29/11/90 29/10/90 02/01/91 06/03/97 08/04/92 20/08/92 07/02/95 05/03/96 18/03/97 15/07/97
WO 9209160 A1	29/05/92	AT 171024 T CA 2095723 A EP 0556305 A,B JP 6501120 T JP 7089345 B US 5103476 A US 5222134 A	15/09/98 08/05/92 25/08/93 27/01/94 27/09/95 07/04/92 22/06/93

Form PCT/ISA/210 (patent family annex) (July 1992)